REMARKS/ARGUMENTS

Status

This paper is submitted under 37 CFR 1.114(c) to accompany a Request for Continued Examination (RCE) filed herewith in response to the Final Office Action mailed April 15, 2008. A Notice of Appeal was mailed on October 15, 2008 with a Certificate of Mailing (37 CFR1.8), and received by the Office on October 20, 2008. An Appeal Brief to the Board of Patent Appeals and Interferences was due no earlier than December 15, 2008. In lieu of the Appeal Brief, Applicant respectfully submits this amendment with the aforesaid RCE, thereby withdrawing the Notice of Appeal previously filed (37 CFR 1.114(d)). A Request for a Four Month Extension of Time under 1.136(a) is submitted herewith, along with the fee prescribed by 37 CFR 1.17(a)(4), extending the time to file this submission to at least April 15, 2009. The response is therefore timely, and reconsideration is respectfully requested.

Claims 20-39 were examined. Claims 30-39 were rejected under 35 U.S.C. §112, first paragraph. Claims 20, 21, 24, 25, 28, 29, 33, 35, and 37 were rejected under 35 U.S.C. §112, second paragraph. Claims 20-23, 26, 33, 34, 38, and 39 were rejected under 25 U.S.C. §103(a) as unpatentable over US 5,754,938 – Herz et al. in view of the Pfitzmann et al. article. Claims 24, 25, 27-31, and 35-37 were rejected under 35 U.S.C. §103(a) as unpatentable over Herz et al. in view of Pfitzmann et al. and in further view of the Engberg et al. article. Claim 32 was rejected under 35 U.S.C. §103(a) as unpatentable over Herz et al. in view of Pfitzmann et al. and Engberg et al. and in further view of US 2006/0155993 – Busboon. In addition, the specification was objected to.

As set forth above, claims 20, 21, 24, 25, 28-31, 33, 35, and 37 have been amended. As explained below, it is respectfully submitted that claims 20-39, as amended, are now in compliance with Section 112 and define patentably over the cited art.

Objection to the Specification

The specification was objected to for failing to provide a proper antecedent basis for "a first identity device," "a second identity device," "a third identity device," and "a further identity device," as recited in one or more of claims 20, 33, 32, and 27.

Antecedent basis for an "identity device" may be found in paragraph 0224 of the Patent Application Publication No. 2007/0106892 (hereinafter the "published application"): "One

aspect of RFID authenticity is the ability to improve authentication of Identity devices such as a MAD-device incorporating a secure chip card combined with the ability to communicate. User authentication towards the MAD is based on passwords, having the physical device, biometrics towards templates etc. and can be augmented with a RFID Tag that the MAD require[s] to be nearby." Additionally, paragraphs 0174-0175 of the published application state: "The preferred solution would be to incorporate the chip card in a dedicated personal authentication device in communication with other devices using wireless protocols. This way the same chip card can be used to control all user devices using privacy device authentication to establish control with the specific device. This can be split into two devices in the form of a Master Authentication Device (dedicated to handling basic keys and physical authentication across devices) authenticated to a Master Communication Device (mobile phone, pda, portable, etc.) handling additional communication."

As discussed in paragraphs 0174-0175 of the published application, an "identity device" may be any Master Authentication Device (MAD) with a secure chip card combined with a Master Communication Device (MCD). Thus, a "first identity device" may be any identity device comprising a MAD, chip card, and MCD utilized by a first entity; a "second identity device" may be any identity device comprising a MAD, chip card, and MCD utilized by a second entity; a "third identity device" may be any identity device comprising a MAD, chip card, and MCD utilized by a third entity; and a "further identity device" may be any identity device comprising a MAD, chip card, and MCD utilized by a further entity. Further, as illustrated in Fig. 10, an MCD may control Specific Master Devices (SMD) and Slave Devices (SD); therefore "identity device" may also (through delegation) include SMDs and SDs.

For example, in Fig. 3, Client 48 may utilize a "first identity device" comprising a MAD, chip card, and MCD to communicate with Financial/Credential Institution 52, which utilizes a "second identity device" comprising a second MAD, chip card, and MCD. Similarly, Shop Computer 44 may utilize a "third identity device" comprising a third MAD, chip card, and MCD to communicate with either Client 48 or Financial/Credential Institution 52.

Rejections under Section 112

Claims 33-39 were rejected under 35 U.S.C. §112, first paragraph, as being based on a disclosure that is not enabling for failure to describe structure to support "means plus function" limitations in the claims. This rejection is respectfully traversed.

Claim 33 was rejected on the grounds that there was no structure in the specification to support "means for verifying the authentication…," and "means for establishing a second path of communication from said one-time-only privacy reference point to a second identity device representing a second legal entity through said data communication network." Applicant respectfully traverses this rejection.

Applicant respectfully submits that structure to support the "means for verifying" limitation is described in paragraph 0174 of the published application, which states: "The preferred solution would be to incorporate the chip card in a dedicated personal authentication device communication with other devices using wireless protocols. This way the same chip card can be used to control all user devices using privacy device authentication to establish control with the specific device." Further support for this limitation is found in paragraphs 0204 and 0205 of the published application.

Applicant respectfully submits that structure to support the "means for establishing a second path of communication" limitation is described in paragraphs 0085-0086 of the published application, which relate to the use of Privacy Reference Points to provide a means for establishing communication without disclosing the identity of the first identity device. Specifically, paragraphs 0085-0086 state: "Whenever a transaction is initiated a PRP is provided by the Chip Card as the transaction specific identifier or one-time-only card number. Except for this identifier the Chip Card will leave NO additional identifiers unless voluntary approved by the Client as part of the transaction. In case of PRPs provided by a RFID-tag as an RFID pseudonym from a list of pseudonyms (such as a ticket) etc. the PRP store pre-encrypted information that upon forwarding to the Service Provider authorize release of data to the provider of services." Further structure supporting this limitation is described in paragraph 0175 of the published application, which states: "This can be split into two devices in the form of a Master Authentication Device (dedicated to handling basic keys and physical authentication across devices) authenticated to a Master Communication Device (mobile phone, pda, portable, etc.) handling additional communication." Still further structure in support of this limitation is

11

believed to be found in Figs. 10 and 14, as described in the paragraphs added to the specification in the amendment filed January 18, 2008.

Claim 37 was rejected on the grounds that there is no structure in the specification to support "means for verifying [that] employs data...." It is respectfully submitted that structure to support this limitation is described in paragraphs 0288-0289 of the published application, wherein it is stated: "In a specific implementation such a TRUSTHW virtual machine is combined with user-specific keys to create a Master Authentication Device (see The Digital Privacy Highway FIG. 10). User-specific keys include the ability for the end-user to authenticate using biometrics, passwords or any interaction towards the MAD device in order to activate the external virtual identity key. A MAD-device may itself contain biometrics readers or make use of a Slave device to read biometrics in order to compare these with stored and hashed templates. Upon match the MAD device can use the advanced revocation control features described in FIG. 11 on Managed Digital Signatures to get access to stored sensitive material such as Digital Signatures or unencrypted certified biometrics still retaining the ability to instantly revoke the MAD-device for any future abuse."

Additionally, further support is described paragraph 521 of the published application, which describes the "Basic Zero-Knowledge Device Authentication Protocol," wherein it is stated: "The core zero-knowledge authenticated request is not generated by the RFID reader itself, but by an actor using any device under his control, which is able to generate a request which is then forwarded to the RFID reader and communicated to the RFID tag. Upon proper authentication the TAG will respond in a similar manner to the RFID reader which returns the reply to the actor, who can then initiate the next step. This can be simply detecting the presence of the specific tag and doing nothing or instructing the Tag to do some operation such as revealing the ePC to a retailer. Normally we would however assume that the actor device itself will handle communication towards third parties and the tag itself only communicates with the actor device ensuring the ePC is NOT stored on the tag."

Claims 20-21, 24-25, 28-29, 33, 35, and 37 were rejected under 35 U.S.C. §112, second paragraph. Claims 24 and 29 were rejected on the grounds of lack of clarity, indefiniteness, and/or ambiguity. Claims 20-21, 24-25, 28-29, 33, 35 and 37 were rejected on the grounds of lack of antecedent basis. These claims have been amended to address the issues raised by the

Examiner. It is believed that the amended claims are sufficiently clear and definite to comply with Section 112, second paragraph, and that proper antecedent bases are provided in every claim. It is therefore respectfully submitted that claims 20-21, 24-25, 28-29, 33, 35, and 37 are in compliance with Section 112.

Rejections under Section 103(a)

Claims 20-23, 26, 33-34, and 38-39 were rejected as unpatentable over Herz et al. in view of Pfitzmann et al. Claims 24-25, 27-31, and 35-37 were rejected as unpatentable over Herz et al. in view of Pfitzmann et al. and in further view of Engberg et al.

Claim 20, as amended, defines a "method of establishing a communication path from a first identity device having an identity representing a first legal entity in a data communication network, comprising the steps of: providing a one-time-only privacy reference point in said data communication network; establishing a communication path from the first identity device to said one-time-only privacy reference point; providing an authentication of said first identity device relative to said one-time-only privacy reference point; verifying the authentication of the first identity device relative to said one-time-only private reference point from said first identity device; and establishing communication from said one-time-only privacy reference point to a second identity device representing a second legal entity through said data communication network; wherein at least one of the steps of verifying the authentication and establishing communication is performed without disclosing the identity of said first identity device."

As Applicant has previously argued, claim 20 relates to and recites first and second "identity devices," and it specifically defines the private reference point as a "one-time-only privacy reference point," indicating that the communication from the first identity device via the network to the second identity device is established via a one-time-only privacy reference point. As discussed in the specification, the one-time-only privacy reference point is a virtual address that is used only once by the first identity device in order to create addressing and prevent any information from being included in the network that could disclose the identity of the first identity device, either as a true identity represented by an address, card number, etc., or as a synonym or pseudonym as suggested by Herz et al. As the privacy reference points are one-time-only, any session would incorporate a new privacy reference point. Therefore, when a shared secret has been established, a first entity using a first identity device and second entity

13

using a second identity device may locate each other using a new connection each time. No information is leaked to the network that this is actually a reconnection of the same pseudonym connecting and linking the first identity device and the second identity device.

The Herz et al. reference, as currently understood by the Applicant, does not appear to teach the use of a one-time-only privacy reference point, nor does it teach a communication path from the first identity device to a one-time-only privacy reference point, as defined in claim 20. Instead, the method of Herz et al. relies on trusted parties (the proxy servers) to anonymize the communication path in order to try to reduce the data leakage that has already occurred between the device and a first proxy server. However, the pseudonym is not disclosed as "one-time-only," nor is it seen how it could function as a "one-time-only" privacy reference point. Moreover, the proxy server knows the true identity of the device connected to it. Therefore, within the network, information is presented that links the pseudonym identity with the true identity, and that may be intentionally or unintentionally leaked to disclose the identity of the first identity device.

Furthermore, the present invention, as defined in claim 20, provides that authentication is made from the <u>first identity device relative to the one-time-only privacy reference point</u>. In other words, it is a purpose-specific authentication without authenticating the device itself. This arrangement prevents data or information that could disclose the identity of the first identity device from being presented or transferred to the network. This is distinct from the system of Herz et al., as currently understood by Applicant, which, even though addressing only anonymous transactions, requires trust in a mixnet. Accordingly, there is no authentication of the device beyond merely verifying a key generated and controlled by the device. The device itself is not identifiable by this key, but, rather, through its leak of identifiers in the communication protocol layer. Thus, as understood by Applicant, the Herz et al. system has no security mechanisms to prevent data or information that could disclose the identity of the first identity device from being transferred to the network. In addition, the Herz et al. system appears (as currently understood by Applicant) to require a mixnet for protection of the device itself, which adds complexity, cost, and battery drain. In the present invention, by contrast, verification and authentication take place in the device itself, and thus do not require a mixnet for device protection. (In the present invention, mixnets are only used in case the location of the gateway,

14

when connecting leaked endpoint identifiers, reveals information such as home location.) The device is thus protected from tracking even in hostile environments even without the use of mixnets. The Herz et al. system, as understood by Applicant, would not protect the device from local tracking in hostile environments.

In addition, the present invention, as defined in claim 20, is distinct from the teachings of Herz et al., in that in the present invention, the communication to the network is established from the one-time-only privacy reference point to the second identity device. In the Herz et al. method, as mentioned above (as currently understood by Applicant), there is no one-time-only privacy reference point, and communication to the network is established from the holder of the first identity device. Specifically, in the Herz et al. method (as currently understood by Applicant), the service provider requires proof that the purchaser has sufficient funds on deposit at a bank or the like. Thus, the Herz et al. method would rely on the safety and security provided by the trusted party (i.e., the proxy server) by transmitting the information relating to the holder as a pseudonym, rather than in clear text. By contrast, in the present invention, as defined in claim 20, the communication is established from the one-time-only privacy reference point to the network after the first identity device has first verified the authenticity of itself relative to the one-time-only privacy reference point from the first identity device itself.

Moreover, claim 20 requires that at least one of the steps of (i) verifying the authentication and (ii) establishing communication is performed without disclosing the identity of the first identity device. Thus, the identity of the first identity device, irrespective of the presentation of the identity in clear text or in pseudonym, is not presented to the network, as the identity is not disclosed to the one-time-only privacy reference point. This is distinct from the Herz et al. method (as currently understood by Applicant), in which the trusted party (the proxy server) includes information linking the pseudonym to the true identity.

In the Final Office Action, it was conceded therein that "Herz is silent about one-time-use pseudonym (i.e. one-time-use reference ('privacy reference point')." Pfitzmann was cited for teaching a one-time-use pseudonym. It was the Examiner's position that it would have been obvious to employ the teaching of Pfitzmann in the method of Herz to provide a different pseudonym for each transaction, with "no possibility to link different transactions by equality of pseudonyms."

15

Herz states: "However, complete privacy and inaccessibility of user transactions and profile summary information would hinder implementation of the system for customized electronic identification of desirable objects and would deprive the user of many of the advantages derived through the system's use of user-specific information ... Indeed, the usefulness of the technology described herein is contingent upon the ability of the system to collect and compare data about many users and many target objects." Herz, column 31, lines 32-46. Additionally, "A second function of the proxy server is to record user-specific information associated with user U. This user-specific information includes a user profile and target profile interest summary for user U, as well as a list of access control instructions specified by user U..." Herz, column 32, lines 34-38. It is improper to combine references where the references teach away from their combination. MPEP §2145. Herz teaches away from the use of a one-time-use transaction pseudonym, as disclosed by Pfitzmann, because the Herz et al. system, as understood by Applicant, requires the ability to collect and compare data about many users and many target objects. In fact, a function of the proxy server in Herz (as understood by Applicant) is to record user-specific information. The combination of a system as disclosed in Herz with a one-time-use transaction pseudonym as disclosed by Pfitzmann would remove the ability of the system in Herz to collect data about users and target objects. The use of one-time-use transaction pseudonyms results in "no possibility to link different transactions by equality of pseudonyms." Pfitzmann, p. 6. Therefore, no data about users or target objects may be linked, and the system in Herz would be unsatisfactory for an intended purpose of customizing electronic identification of desirable objects. Thus, it appears that it is improper to combine Herz and Pfitzmann as suggested in the Office Action. Accordingly, it is respectfully submitted that claim 20 is allowable, as are dependant claims 21-32.

Claim 33, as amended, specifies "A system for establishing a communication path from a first identity device in a data communication network, comprising: a one-time-only privacy reference point in said data communication network; a first communication path defined from said first identity device to said one-time-only privacy reference point; means for providing an authentication of the first identity device relative to said on-time-only privacy reference point; means for verifying the authentication of said first identity device relative to said one-time-only privacy reference point from said first identity device; and means for establishing a second path

of communication from said one-time-only privacy reference point to a second identity device through said data communication network; wherein at least one of the means for verifying the authentication and the means for establishing communication is operable without disclosing an identity of said first identity device to said second identity device"

Claim 33 was rejected on the same basis as claim 20. Herz et al., as currently understood by Applicant, is patentably distinct from the invention defined in claim 33, for the reasons given above with respect to claim 20. Furthermore, as discussed above, it is submitted that Herz teaches away from the use of one-time-only transaction pseudonyms as disclosed by Pfitzmann. It is therefore improper to combine Herz with Pfitzmann for the reasons set forth above. Accordingly, it is respectfully submitted that claim 33 is allowable for the same reasons discussed above with regard to claim 20, as are dependant claims 34-39.

It is thus respectfully submitted that, for the reasons set forth above, independent claims 20 and 33 are neither anticipated nor rendered obvious by Herz et al., taken singly or in any combination with Pfitzmann that might have reasonably suggested itself to those of ordinary skill in the pertinent arts at the time the claimed subject matter was invented. Furthermore, nothing in either the Engberg reference or the Bushboon reference, taken in any combination with the disclosures of Herz et al. and Pfitzmann that might reasonably have suggested itself to those of ordinary skill in the pertinent arts, would teach or suggest the subject matter defined in claims 20 and 33. Therefore, it is respectfully submitted that claims 20 and 33 define patentably over the art of record and should be allowed.

Claims 21-32 depend from claim 20, and claims 34-39 depend from claim 33. These dependent claims further define, with greater particularity, the various novel and non-obvious aspects and features of Applicant's invention, and should therefore be allowed along with their respective independent claims.
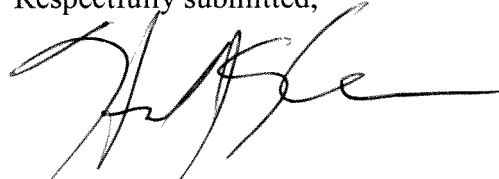
///

///

///

17

In summary, it is respectfully submitted that claims 20-39 define patentably over the art of record and should be allowed. Passage of the application to issue is therefore earnestly solicited.

Respectfully submitted,

Date:  April 15, 2009

HOWARD J. KLEIN
Registration No. 28,727

Klein, O'Neill & Singh, LLP (Customer No.: 22145)
43 Corporate Park
Suite 204
Irvine, CA 92606
Tel: (949) 955-1920
Fax: (949) 955 1921